Health Budgets & Financial Policy

TMA Uniform Business Office

Privacy and HIPAA Security

15 December 2009 - 0800 & 1000

17 December, 2009 - 0800 & 1600

Bridge Number: 877-960-7130

Pin: 2378585

Health Budgets & Financial Policy

TMA Uniform Business Office

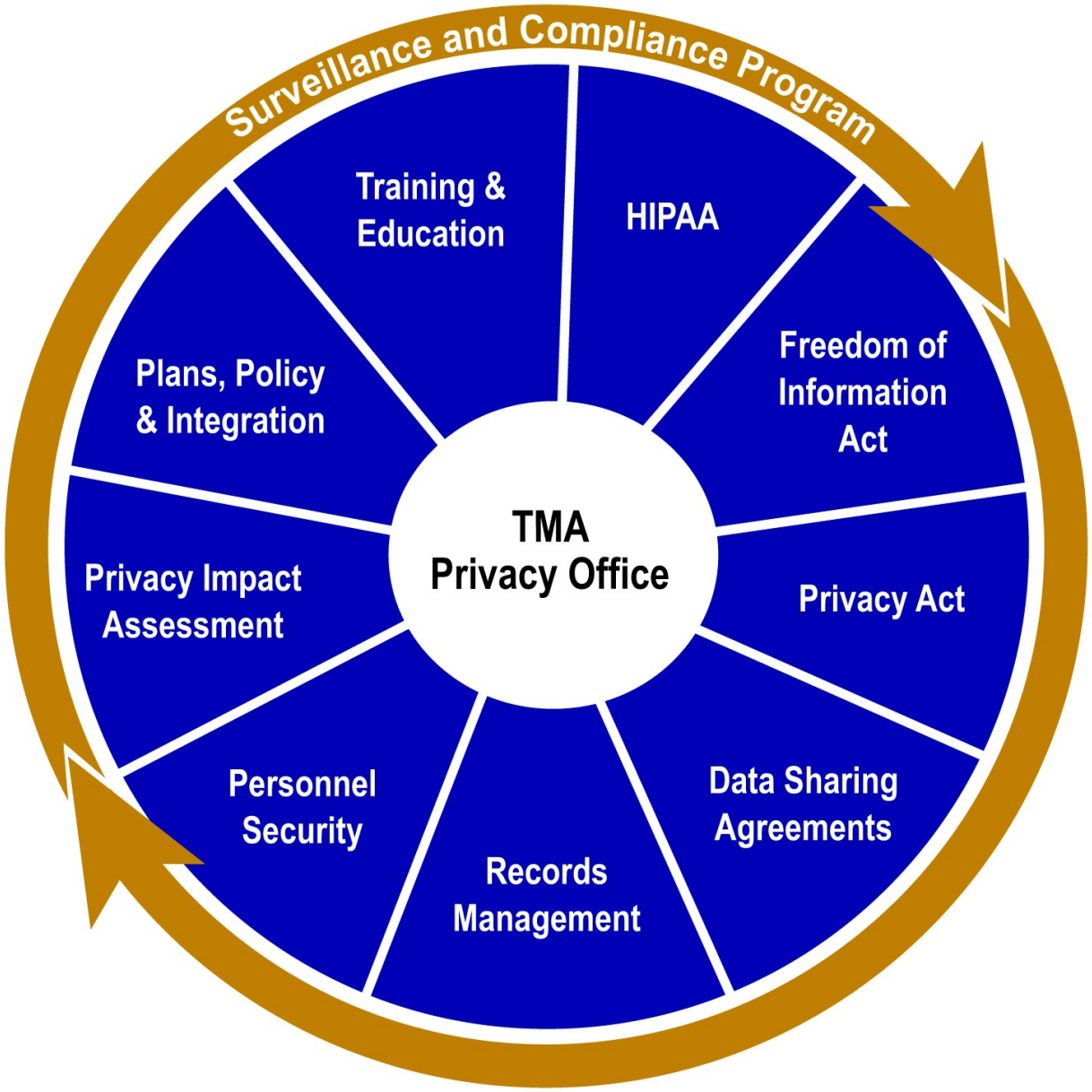
Privacy and HIPAA Security

Objectives

This course focuses on the requirements for both the **Privacy Act** and **HIPAA**. In compliance with **DoD 5400.11-R**, "DoD Privacy Program", this course covers the following topics:

Health Budgets & Financial Policy

TMA Uniform Business Office



Health Budgets & Financial Policy

Definitions You Should Know….

Workforce

TMA Uniform Business Office

DoD 6025.18-R, DoD Health Information Privacy Regulation" defines the workforce as:

- Employees, volunteers, trainees, and other persons whose conduct, in performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity

The **Privacy Act** recognizes that contractors and other non-DoD personnel who work on behalf of the Department may access and use PII/PHI on behalf of the organization. **HIPAA** refers to these contractors as Business Associates (BA).

Health Budgets & Financial Policy

Definitions You Should Know….

Business Associates and Contractors

TMA Uniform Business Office

- According to the DoD Privacy Program, any contractor who may come in contact with PII/PHI will be recognized as employees of DoD, and therefore, they must be trained in the proper handling and protection of PII/PHI. Records created and used by the contractor may be subject to the **FOIA,** the **Privacy Act,** and **HIPAA.**

- In addition to the training, the contract must have a Business Associate Agreement (BAA) as required by HIPAA. This agreement provides guidance and documentation as to the BA's responsibilities in protecting PHI.

Health Budgets & Financial Policy

Definitions You Should Know….

Personally Identifiable Information (PII)

TMA Uniform Business Office

DoD 5400.11-R defines PII as “information which can be used to distinguish or trace an individual’s identity.”

PII includes:

- Name
- Social Security Number
- Age
- Date and place of birth
- Mother’s maiden name
- Biometric records
- Marital status
- Military Rank or Civilian Grade
- Race
- Salary
- Home/office phone numbers
- Other personal information including health information, which can be linked to a specific individual

Health Budgets & Financial Policy

TMA Uniform Business Office

Definitions You Should Know….

Protected Health Information (PHI)

PHI includes the following individually identifiable data elements, **when combined** with health information about that individual:

- Names
- All geographic subdivisions smaller than a state
- All elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/License numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, code, or combination that allows identification of an individual

Health Budgets & Financial Policy

Definitions You Should Know…

Minimum Necessary Standard

TMA Uniform Business Office

The <u>Minimum Necessary Standard</u> states that an organization should limit the use or disclosure of PHI to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

Health Insurance Portability and Accountability Act, 1996

The **Privacy Act** requires that an organization use and store only the minimal information that is relevant and necessary for each individual in its SOR.

HIPAA further defines this requirement to limit all disclosures of PHI, including any made for payment and/or health care operations, only to the minimum necessary needed. In **HIPAA,** this requirement is referred to as the **Minimum Necessary Standard.**

It is important to note that this standard does not apply to any disclosure of PHI for treatment purposes. For questions or doubts about sharing data, contact a supervisor or the local Privacy Officer.

Health Budgets & Financial Policy

Definitions You Should Know…

De-Identified PHI

TMA Uniform Business Office

De-identified PHI is data that ***excludes*** the following **18** categories of direct identifiers of the individual or of relatives, employers, or household members of the individual:

De-Identified PHI	
▪ Names ▪ All geographic subdivisions smaller than a State ▪ All elements of dates (except year) ▪ Telephone numbers ▪ Fax numbers ▪ Electronic mail addresses ▪ Social Security Numbers ▪ Medical Record numbers ▪ Account numbers ▪ Health plan beneficiary numbers ▪ Certificate or license numbers	• Internet protocol (IP) address • Device identifiers and serial numbers • Web universal resource locators (URLs) • Biometric identifiers, including finger and voice prints • Vehicle Identification Numbers and License Plate Numbers • Full-face photographic images and comparable images • Any other unique, identifying characteristic or code, except as permitted for re- identification in the HIPAA Privacy Rule

Health Budgets & Financial Policy

Definitions You Should Know…

Limited Data Sets

TMA Uniform Business Office

Limited data sets have defined uses and disclosures. **Under HIPAA, only three purposes are allowed for limited data sets**: research, public health, or health care operations

A limited data set is PHI that ***excludes*** **16** categories of direct identifiers of the individual or of relatives, employers, or household members of the individual

However, unlike de-identified data, there are more restrictions as to who can receive this data and it requires that the recipient agree to not to attempt to re-identify any of the data

Health Budgets & Financial Policy

Definitions You Should Know…

Limited Data Set (LDS)

TMA Uniform Business Office

A limited data set is PHI that ***excludes*** the following **16** categories of direct identifiers of the individual or of relatives, employers, or household members of the individual:

PII Direct Identifiers	
• Names • Address other than town, city, state, and zip code • Telephone numbers • Fax numbers • Electronic mail addresses • Social Security Numbers • Medical Record numbers • Account numbers • Health plan beneficiary numbers • Certificate/license numbers	• Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web universal resource locators (URLs) • Internet protocol (IP) address • Biometric identifiers, including finger and voice prints • Full-face photographic images and comparable images

Health
Budgets &
Financial
Policy

TMA
Uniform
Business
Office

Workforce Responsibilities

Health Budgets & Financial Policy

TMA Uniform Business Office

Workforce Responsibilities

Workforce Access to PII/PHI

- The workforce may have access to all categories of PII/PHI. All PII/PHI must be handled with the appropriate level of care and protection.
- Workforce access to PII/PHI is restricted to what is necessary to complete a work-related duty or job. This "minimum necessary standard" is based on the need-to-know and the need to perform assigned duties and responsibilities.
- The minimum necessary standard does not apply to the following:
  - Disclosures to or requests by a healthcare provider for treatment.
  - Uses and disclosures made to the individual.
  - Uses and disclosures made after an individual's authorization has been granted.
- **If using a DoD information system with access to PII/PHI, security and awareness training must be completed prior to account set-up.**

Health Budgets & Financial Policy

Workforce Responsibilities

Guidelines for PII/PHI

TMA Uniform Business Office

- Know what PII/PHI is available in your environment and how it can be accessed.
  - Know how and where hard copy files are stored.
  - Create and maintain an inventory of all documents that contain PII/PHI.
  - Keep a list of employees who have access to PII/PHI, paper and electronic.
- Control how much PII/PHI is maintained in your area.
  - Limit the amount of PII/PHI to what is needed to reduce the risk of information being used inappropriately.
  - If the information is no longer needed, get written authorization from your supervisor to have the files moved to storage or destroyed (i.e., shred or burn).
- Ensure all PII/PHI is protected from casual or unintentional disclosure.
  - Use locks, storage rooms, and computer controls.
  - Position fax machines and computer screens so they are away from heavy traffic and public access.
  - Be aware of surroundings when using a cell phone and/or BlackBerry®.
  - Lock the computer when away from the desk.
- Follow local policies and procedures for handling PII/PHI.

Health Budgets & Financial Policy

TMA Uniform Business Office

Workforce Responsibilities

Using and Disclosing PII/PHI

- The disclosure of PII/PHI refers to the sharing of information. These disclosure guidelines apply to all forms of PII/PHI, including verbal, paper, and electronic.
- Workforce access and disclosure of PII/PHI for the purposes of treatment, payment, and healthcare operations (TPO) is permitted without signed authorization from the individual.
- Some ways to minimize incidental disclosures:
  - Refrain from discussing information in public places
  - Protect computer screen from public view
  - Observe the “Minimum Necessary” Standard when sharing and relating information

Health Budgets & Financial Policy

Workforce Responsibilities

Transmitting PII/PHI

TMA Uniform Business Office

- PII/PHI can be transmitted between facilities by methods that include the use of email and fax.
  - Before the transmission of PII/PHI, contact your supervisor to ensure the information is being sent encrypted.
  - Do not send PII/PHI to unknown sites or facilities.
  - Use only DoD authorized information systems, networks, and applications.
  - Transmit PII/PHI using remote access only with prior approval.
  - Use your CAC to log-in and off from your workstation and to encrypt emails containing PII/PHI

Health Budgets & Financial Policy

Workforce Responsibilities

Transporting PII/PHI

TMA Uniform Business Office

When necessary, PII/PHI can be physically transported between approved locations with a supervisor's authorization, when electronic means are not appropriate.

- Obtain authorization from a supervisor before transporting PII/PHI.
- Use passwords to protect networks and laptops that contain PII/PHI.
- Contact your supervisor to ensure that portable media, including laptops, PDAs, USB flash drives (thumb drives), and compact discs (CDs) are encrypted.
- Enforce "strong password rules" (alpha/numeric, special characters, and at least 8 characters).
- Do not allow employees to "share" passwords.
- Wrap all PII/PHI in envelopes or wrappings before transporting outside of TMA buildings. Envelopes should be:
  - Opaque
  - Strong and durable
  - Able to prevent unintentional disclosure during transit
  - Clearly marked, including name and destination address
- Ensure there is a tracking process in place for the transportation of PII/PHI, whether in paper records or CDs/media devices, and that accountability be strongly emphasized with the establishment of this process.

Health Budgets & Financial Policy

Workforce Responsibilities

Storing PII/PHI

TMA Uniform Business Office

- **Storing Paper PII/PHI**
  - Paper storage must be secured under lock and key when unattended.
  - Documents must be covered or in folders if there are visitors around your work area.
- **Storing Electronic PII/PHI**
  - Ensure your computer has virus protection installed.
  - Maintain a record of personnel with access to hardware and software containing PII/PHI.
  - Lock unattended laptops.
  - Use passwords to protect files and all portable or remote devices.
  - Contact your supervisor to ensure the use of encryption on all portable or remote devices, including laptops, thumb drives, PDAs, and CDs. *(Please refer to the "Warning" graphic above Section 7 regarding the current policy on the use of portable media in DoD systems)*
  - Do not download PII/PHI onto remote systems or devices without approval.

Health Budgets & Financial Policy

Workforce Responsibilities

Destroying PII/PHI

TMA Uniform Business Office

- Prior authorization must be issued before deleting or destroying any stored PII/PHI from local file directories, networks, removable devices, or paper files.
- PII/PHI that meets the definition of a record, regardless of media, shall be destroyed by the appropriate method in accordance with DoD Administrative Instruction 15, Records Management and current preservation orders.
- PII/PHI that is no longer required for operational purposes must be destroyed completely to prevent recognition or reconstruction of the information.
- Non record PII/PHI may be destroyed at any time. PII/PHI that meets the definition of a record, regardless of media, shall be destroyed by the appropriate method in accordance with DoD Administrative Instruction 15, Records Management and current preservation orders.

Health
Budgets &
Financial
Policy

TMA
Uniform
Business
Office

Non-Compliance

Health Budgets & Financial Policy

Non-Compliance

Remedies and Penalties

TMA Uniform Business Office

The **Privacy Act** and **HIPAA** allow penalties to be imposed upon organizations or individuals who, through intent or neglect, disclose PII/PHI inappropriately.

Penalties against individuals may include fines, sanctions, termination of employment, and in some cases, prison terms.

Penalties against organizations may include fines, sanctions, and termination of contracts.

Both the **Privacy Act** and **HIPAA** also establish processes by which individuals may seek **administrative** and **civil remedies**.

Health Budgets & Financial Policy

TMA Uniform Business Office

Non-Compliance

Non-Retaliation for Whistleblowers

- Employees are expected to report any issues or concerns about protecting patients' privacy to their immediate supervisors who will report up the chain of command
- Managers must support employees to do the right thing in protecting patient information
- Managers may not punish employees for reporting known or suspected cases of others breaking privacy and security rules

Health
Budgets &
Financial
Policy

TMA
Uniform
Business
Office

Evolving Threats

Health Budgets & Financial Policy

TMA Uniform Business Office

Evolving Threats

Health
Budgets &
Financial
Policy

TMA
Uniform
Business
Office

Summary

Health Budgets & Financial Policy

Best Practices

TMA Uniform Business Office

To safeguard data and prevent breaches, **DO** (1 of 2)

- Remove your Common Access Card (CAC) from your computer to prevent unauthorized access to data
- Ensure that your notes and working papers that may contain PII/PHI are shredded or put in a burn bag
- Make certain that filing cabinets are purged of information prior to moving or disposal
- Verify that e-mail extensions make sense
- Always use a cover sheet with a confidentiality disclaimer statement when sending faxes

Health Budgets & Financial Policy

Best Practices

TMA Uniform Business Office

- To safeguard data and help prevent breaches, **DO** (2 of 2)
  - Avoid clicking on links sent in unsolicited emails
  - Challenge “anyone” who asks to see PII or PHI for which you are responsible and determine if they have a need to know
  - Prevent anyone looking over your shoulder when you are accessing PII/PHI
  - Refrain from sharing your passwords/Personal Identification Numbers (PINs) with anyone

Health
Budgets &
Financial
Policy

TMA
Uniform
Business
Office

QUESTIONS